Senator Feinstein to Introduce Tougher ID Theft Notification Bill

April 11, 2005

Washington, DC – In light of numerous recent data breaches, U.S. Senator Dianne Feinstein (D-Calif.) will today introduce strengthened identity theft legislation that would ensure that consumers are notified when their personal information is compromised.

"Every day, we learn that we are more and more at risk from identity theft – entire databases have been lost, stolen, or hacked into it," Senator Feinstein said. **"First, we heard about ChoicePoint – a case that resulted in the theft of the personal information of 145,000 Americans – but this was just the beginning. Now we have watched as wave after wave of data system theft has come to light, exposing millions of Americans to identity theft.**

"The fact of the matter is that your buying habits, your bank accounts, your Social Security number, your driver's license – all of your personal data – today is being collected, collated, distributed, bought, sold – without your knowledge or consent. So what can we do? We desperately need a strong national standard that says whenever a data system is breached, everyone who is at risk of identity theft must be notified."

"I first introduced legislation to do this in the 108th Congress and then again on the first day of the 109th. But after additional discussions with privacy rights advocates, it became clear that much more needed to be done to protect Americans."

Senator Feinstein worked with representatives from Consumers Union, the Privacy Rights Clearinghouse, and other privacy-rights groups to strengthen her legislation and develop this strong national standard for notification. The Senate Judiciary Committee will hold a hearing examining this bill on April 13, 2005.

Summary

The bill requires a business or government entity to notify an individual in writing or email when it is believed that personal information – such as a Social Security number, driver's license or state identification number, or credit card or bank account information – has been compromised.

Only two exceptions to notification exist. First, upon the written request of law enforcement for purposes of a criminal investigation; and second, for national security purposes.

In cases where written or e-mail notice is not possible due to the cost or number of individuals to be notified, substitute notice is acceptable. However, in order to qualify for substitute notice, the government or business must demonstrate that the cost of providing direct notice would exceed $500,000 or 500,000 individuals to be notified. Substitute notice allows for

notice to be done by an internet website posting or media release. Written or e-mail notice can also be substituted if the government agency or business does not have sufficient contact information to properly notify individuals.

The bill is based on the ground-breaking California law is the first and only State law requiring notification of individuals. But in fact, the legislation is stronger than the California law:

- It covers both electronic and non-electronic data – as well as encrypted and non-encrypted data. The California law only includes unencrypted, electronic data.

- It allows individuals to put a 7-year fraud alert on their credit report. The California law doesn't address fraud alerts.

- It doesn't include a major loophole allowing companies to follow weaker notification requirements – as the California law does.

- It lays out specific requirements for what must be included in notices, including:

    - a description of the data that may have been compromised;
    - a toll-free free number to learn what information and which individuals have been put at risk;
    - and the numbers and addresses for the three major credit reporting agencies.

- By contrast, California law is silent on what should be in notices.

- It has tougher civil penalties -- $1,000 per individual they failed to notify or not more than $50,000 per day while the failure to notify continues or existed. In California, a victim may bring a civil action to recover damages or the company may be enjoined from further violations.

- And it sets a national standard – so that individuals in Iowa, Oklahoma, and Maine have the same protections as consumers in California.

- The law would be enforced by the Federal Trade Commission or other relevant regulator, or by a State attorney general who could file a civil suit.

Recent breaches

- **Data Processors International** – a database of 8 million credit card records was breached by hackers in February 2004.

- **UCLA Blood Center** – a laptop containing the Social Security Numbers of 145,000 blood donors was stolen in June 2004.

- **ChoicePoint** – personal information from 145,000 Americans was sold to an identity theft ring posing as a legitimate business in September 2004. ChoicePoint had a similar breach in 2002, involving about 7,000 records.

- **UC Berkeley** – a database containing the Social Security Numbers and dates of birth of 600,000 students, faculty and alumni was hacked in October 2004.

- **Also at UC Berkeley --** a laptop containing the Social Security Numbers and other identifying information of 98,000 students, alumni, and applicants was stolen from an unlocked office in March 2005.

- **UC San Francisco** – a computer containing the Social Security Numbers of 7,000 students, faculty, and staff was hacked in April 2005.

- **George Mason University** – 30,000 photographs and Social Security Numbers were compromised by hackers in January 2005.

- **SAIC** – Laptops containing the Social Security numbers and other private information of 45,000 employees were stolen during a break-in in February 2005.

- **Bank of America** – backup computer tapes containing the records of over 1.2 million people disappeared in February 2005. Those affected included U.S. Senators and Representatives.

- **Boston College** –120,000 alumni's addresses and Social Security Numbers were compromised by hackers in March 2005.

- **LexisNexis** – Identity thieves used stolen passwords to access the Social Security Numbers, driver's licenses and consolidated public records of 32,000 American in March 2005.

- **DSW Shoe Warehouse** – hackers compromised customer databases in 103 shoe stores, gaining access to the credit cards of hundreds of thousands of people in March 2005.

- **San Jose Medical Group** – computers containing the medical records of 185,000 current and former patients were stolen in March 2005.

###